NorSIS
Norsk senter for informasjonssikring

Forsvarsdepartementet

Gjøvik, 20. januar 2017

Vår ref.: 2017-04/BM

Deres ref.: 2015/3139-7/FD V 3/MAY

Oversendelse av høringssvar for NOU 2016:19

Innledning

NorSIS viser til høringsbrev for *NOU 2016:19 Samhandling for sikkerhet – beskyttelse av grunnleggende samfunnsfunksjoner.*

Vi berømmer utvalget for et svært grundig arbeid og mener at utredningen gir et svært godt grunnlag for en nødvendig oppdatering av Sikkerhetsloven. NorSIS er spesielt tilfreds med at utvalget er tydelig i sin beskrivelse av nasjonal samhandling som et sentralt virkemiddel for å møte de sikkerhetsmessige utfordringene.

NorSIS har bemerkninger til delene om lovens virkeområde og til delene om informasjonsdeling.

Lovens virkeområde

Utvalget skriver i punkt *2.1 Lovens virkeområde* at begrepet *grunnleggende nasjonale funksjoner* skal benyttes for å beskrive lovens virkeområde. Det skal være statens oppgave å beslutte hva som utgjør de grunnleggende nasjonale funksjonene.

NorSIS støtter i utgangspunktet at lovens virkeområde endres slik utvalget beskriver, men mener at det er en fare for at virkeområdet blir for snevert i forhold til det som NorSIS oppfatter som nasjonale utfordringer.

NOU 2015:13 Digital sårbarhet – sikkert samfunn beskriver inngående hvordan den digitale omstillingen endrer tilbringelsen av produkter, tjenester og funksjoner. Kritiske samfunnsfunksjoner er avhengige av et nettverk av systemer, tjenester og funksjoner på en slik måte at det vanskelig lar seg gjøre å kartlegge disse avhengighetsforholdene nøyaktig. Vi må også anta at avhengighetene er dynamiske og endrer seg over tid, noe som gjør utfordringen enda større. NorSIS er enig i utvalgets vurdering om at en trussel-aktør vil forsøke å ramme det svakeste leddet. Derfor vil etterretning, påvirkning eller sabotasje mot virksomheter som inngår i et nettverk som de grunnleggende nasjonale funksjonene er avhengig av, kunne føre til alvorlige konsekvenser for de kritiske samfunnsfunksjonene. Kompleksiteten i disse avhengighetsforholdene gjør det svært krevende å kartlegge dem på forhånd.

Post-og besøksadresse
Postboks 85
2801 Gjøvik

Tlf.: +47 4000 5899
Org.nr. 995 195 003

E-post: post@norsis.no
Nett: www.norsis.no

I punkt *6.2.2 Grunnleggende nasjonale funksjoner*, beskrives landets økonomiske frihet og velferd som en grunnleggende forutsetning for Norges evne til å ivareta egen sikkerhet. Utvalget viser til at anslag mot virksomheter som har en sentral rolle i nasjonens økonomi, for eksempel innen petroleumsindustrien, vil kunne ha en vesentlig negativ innvirkning på nasjonens evne til å opprettholde økonomisk trygghet.

NorSIS minner om at de fleste bedrifter i Norge er små- og mellomstore, med 100 ansatte eller færre, og som står for over halvparten av nasjonens BNP. Tradisjonelt har denne gruppen ikke blitt prioritert hva gjelder statens tiltak innen forebyggende digital sikkerhet. NorSIS mener imidlertid at staten nå må ta et større ansvar for å legge til rette for at også disse virksomhetene har tilfredsstillende evne til å iverksette tiltak med hensyn på forebyggende sikkerhet.

NorSIS er enig i utvalgets forslag om å lovfeste en plikt for Nasjonal sikkerhetsmyndighet til å legge til rette for og koordinere at nødvendig informasjon gjøres tilgjengelig for virksomheter og myndigheter som omfattes av loven.

Lovens virkeområde bør imidlertid formuleres slik at loven tydeliggjør statens ansvar for den forebyggende digitale sikkerheten for alle virksomheter i det private næringsliv i Norge. Loven bør følge opp med konkrete tiltak som fremmer forebyggende digital sikkerhet for hele næringslivet.

Informasjonsdeling

Utvalget skriver i punkt *7.7.5 Informasjonsdeling* at tilgang til tidsriktig og relevant informasjon om trusler er en grunnleggende forutsetning for at virksomheter skal kunne gjøre en tilfredsstillende risikovurdering, og å iverksette riktige og forsvarlige sikkerhetstiltak. NorSIS støtter denne vurderingen, og minner om at digitale trusler rammer hele samfunnet.

En fjerdedel[1] av norske virksomheter har opplevd uønskede sikkerhetshendelser det siste året, mange med produktivitetstap og økonomiske tap som konsekvens. I 2014 estimerte Næringslivets sikkerhetsråd de nasjonale kostnadene ved datakriminalitet til 19 milliarder[2]. NorSIS erfarer at norske bedrifter utsettes for spionasje, sabotasje, utpressing og annen datakriminalitet som koster samfunnet store beløp. I 2016 har det eksempelvis vært en økning i såkalt direktørsvindel, der en enkelt virksomhet i følge politiet ble svindlet for 100 millioner. Hvor stort det økonomiske tapet av datakriminalitet er i 2016 er ikke kartlagt, men NorSIS antar at det er på samme nivå eller høyere enn estimatet fra 2014 viser. De mer indirekte konsekvensene av et omfattende tyveri av informasjonsverdier fra norske selskaper er heller ikke kartlagt, men NorSIS mener at det er grunn til å frykte at norsk økonomi vil kunne ta alvorlig skade dersom datakriminaliteten ikke begrenses. Det er vesentlig at næringslivet får tilgang på informasjon som gjør det mulig å iverksette tiltak som beskyttelse mot datakriminalitet.

---

[1] Næringslivets sikkerhetsråd – Mørketallsundersøkelsen 2016

[2] Næringslivets sikkerhetsråd – Mørketallsundersøkelsen 2014

NorSIS anbefaler at loven pålegger norske sikkerhetsmyndigheter å dele informasjon om trusler, sårbarheter og sikringsmetoder i langt større grad enn det som er dagens praksis. Et system basert på sikkerhetsgradering av informasjon og sikkerhetsklarering av personell, kan ikke stå i veien for at norske virksomheter i både privat og offentlig sektor får tilgang til informasjon som er nødvendig for at de skal kunne sikre seg selv på en tilfredsstillende måte.

Oppsummering

NorSIS oppfatter det slik at næringslivet hovedsaklig ikke er underlagt sektorer som har etablerte strukturer[3] for å motta, analysere og formidle trusselinformasjon fra sikkerhetsmyndighetene. Dette mener NorSIS at det må tas høyde for i loven, og at det trolig innebærer en utvidelse av forståelsen til samvirkeprinsippet. Det er etter NorSIS' syn en grunnleggende forutsetning for beskyttelsen av nasjonens økonomi og velferd at loven går langt nok i å bidra til beskyttelse av alle virksomheter i Norge.

Peggy Sandbekken Heie
Administrerende direktør
Norsk senter for informasjonssikring

[3] For eksempel CERT, CSIRT, IRT eller andre varslings- og håndteringsenheter.